I.   REAL PARTY IN INTEREST (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in this application is the assignee, EMC Corporation, a Massachusetts corporation having a place of business at 171 South Street, Hopkinton, Massachusetts 01748.

II.   RELATED APPEALS AND INTERFERENCES (37 C.F.R. §41.37(c)(1)(ii))

There are no other appeals or interferences known to the Applicant, the Applicant's legal representative, or the assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in an appeal.

III.   STATUS OF CLAIMS (37 C.F.R. §41.37(c)(1)(iii))

There are 32 total claims in this application (3 independent claims and 29 dependent claims).   The following list summarizes the status of the claims:

1. Claims pending: 1-4, 6-27 and 29-34
2. Claims rejected: 1-4, 6-27 and 29-34
3. Claims allowed: none
4. Claims withdrawn from consideration: none
5. Claims canceled: 5 and 28

IV.   STATUS OF AMENDMENTS (37 C.F.R. §41.37(c)(1)(iv))

This Response is the sole Response filed subsequent to the Final Office Action mailed on April 21, 2006. There are no unentered amendments.

V.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R.§41.37(c)(1)(vi))

The grounds of rejection to be reviewed on appeal are:

A. The rejection of claims 1-4, 9-27, 29-32 under 35 U.S.C. §103 as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545) and in further view of Boggs (U.S. Patent No. 5,959, 994).

VI.   ARGUMENT (37 C.F.R. §41.37(c)(1)(vii))

A. The Combination of Ericson and Yu is Improper

The Office Action mailed April 21, 2006 (4/21 Office Action) rejects claims 1-4, 9-27 and 29-32 under 35 U.S.C. 103(a) as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545) and in further view of Boggs (U.S. Patent No. 5,959, 994). Applicant respectfully traverses this rejection.

i. The Office Action Fails to Establish a Prima Facie Case of

Obviousness

MPEP §2142 states, "[t]o establish a *prima facie* case of obviousness...there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." The legal concept of *prima facie* obviousness allocates the initial burden of producing factual support to the Examiner (MPEP §2142). In particular, the Examiner bears the initial burden of establishing that there is some suggestion or motivation to combine the references.

The Examiner has failed to produce evidence from the references or elsewhere to support the allegation that there is motivation to combine Ericson and Yu. In the "Response to Arguments" section in the final Office mailed on September 19, 2005 (9/19 Office Action), the 9/19 Office Action asserts that "both Ericson and Yu are directed to improving access security, hence they are analogous art." During a telephone conference conducted on November 15, 2005, the Examiner re-asserted this position, further alleging that since both Ericson and Yu involve access security in a network environment, it would have been obvious to use the authentication measures described in Yu to improve the access security of Ericson. However, even if it is true

1045630.1

that Ericson and Yu are in the same field, that alone does not prove motivation to combine the references.

The Office Action must show incentive to combine the teachings of the two references. In *Ex parte Skinner* (Decision of the Board of Patent Appeals and Interferences,. No. 650-69), the Board stated that "[w]hen the incentive to combine the teachings of the references is not readily apparent, it is the duty of the examiner to explain why the combining of the reference teachings is proper." The Office Action fails to provide any evidence that Yu's authentication methods actually *would* improve the security of Ericson. Not all networks are the same, nor do they exhibit the same security concerns. A security measure taken in one environment may be entirely irrelevant in another, and may not improve security, but rather may be an unnecessary design implementation.

In the "Response to Arguments" section of the 4/21 Office Action, the Office Action notes that Ericson reports that other protocols such as Fibre Channel may be used to implement the invention disclosed in Ericson. The Office Action asserts that the mention of the Fibre Channel protocol is evidence that Ericson describes a system for use in untrusted networks, and therefore the authentication methods of Yu would be expected to improve the security in Ericson. However, the mere mention of a network protocol that is sufficiently generic that it could be used in other system configurations that are untrusted does not somehow override Ericson's teaching (discussed further below) that the disclosed system is intended for use in a trusted environment wherein identity spoofing is not a concern. Accordingly, the contention that the authentication methods of Yu would have somehow improved the security of the network storage system of Ericson is entirely unsupported.

To establish a *prima facie* case of obviousness, it must be shown *why* one skilled in the art, viewing the references at the time of the invention, would have been motivated to add Yu's authentication into Ericson (*Ex parte Skinner*). Accordingly, the Office Action has the burden of showing why one skilled in art would have believed that authentication would have improved security in the Ericson system. Merely stating that Yu's authentication would have improved the security of Ericson without factual support from the references is not sufficient to meet the

1045630.1

Office Action's burden. Accordingly, the Office Action has not established a *prima facie* case of obviousness, and the rejection is therefore improper.

ii. *There is No Motivation to Combine Ericson and Yu.*

As discussed above, the Office Action has failed to meet the burden of showing motivation to combine Ericson and Yu. Therefore, Applicant need not produce evidence to the contrary (MPEP §2142). However, even though Applicant is not obligated to show why it would not have been obvious to combine Ericson and Yu, Applicant provides below support from the references showing that the authentication techniques of Yu would not in fact improve the security of Ericson, so that one skilled in the art would not have been motivated to modify Ericson as alleged in the Office Action because it would have merely complicated the system with unnecessary measures that do not improve security.

a. *Discussion of Ericson*

Ericson is directed to controlling access to a target device 102 (e.g., a disk array) by initiators 100 interconnected by a small computer system interface bus ("SCSI bus") 104, wherein the network devices are preconfigured in accordance with the SCSI specification. (Col. 3, lines 48-56). The initiators 100 request access to the target 102 by directing an access message to the target 102 via the SCSI bus 104, the message including the initiator identifier, a target identifier and a portion of the target device 102 to be accessed (i.e., the logical unit 108). (Col. 3, lines 56-61). Access to the target device is controlled by a look-up structure preconfigured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. When an initiator requests access, the look-up structure is indexed to check whether the initiator has been authorized to access the logical unit identified in the access message before allowing the initiator to access the logical unit (Col. 2, lines 26-65).

b. *Discussion of Yu*

Yu is directed to distributed security measures in an intelligent network having a plurality of interconnected network nodes, each having specified resources (e.g., a distributed telecommunication network architecture). The various nodes store objects associated with network resources having sets of interface operations describing the services provided by the

1045630.1

respective object. Nodes can access the network resources of an object through the invocation of the service elements of the interface of the corresponding object. (Col. 5, lines 1-11). Objects can be identified and protected using a mechanism called a capability. A capability is a unique identifier of an object and a permission that gives a node the right to access the object. When a node requests a service provided by an object residing at another node (referred to as the execution node), a capability for the object is returned to the requesting node, giving it access to the services in the object permitted by the capability. (Col. 5, line 62 – Col. 6, line 11).

With the intelligent network architecture, outside service providers can access service elements of the telephone network. Yu teaches that in a distributed architecture, protection mechanisms for network security and integrity should themselves be distributed, but that if so they are vulnerable to forgery, theft, modification or destruction. (Col. 4, lines 37-65). Because an intruder in such a distributed network can forge almost all parts of a transmitted message except the node address (e.g., the network interface hardware or other low level control), Yu teaches that unique encryption keys be exchanged between an execution node and a node requesting a capability from the execution node, based on the low level hardware address (Col. 6 line 34 – col. 8 line 60). If a capability cannot be decrypted using the unique pairing of keys, the execution node knows that the capability has been tampered with, or an imposter node transmitted the capability of another node. (Col. 7 line 45 – col. 8 line 60).

c.   Trusted and Untrusted Environments

From a security standpoint, the networks described in Ericson and Yu are very different and therefore exhibit different security concerns. In particular, as discussed below, Ericson describes a networked data storage system operating in a trusted environment. Yu describes a network for providing various services in an untrusted environment. A trusted network environment is one wherein devices seeking access to a resource are trusted not to spoof (or are incapable of spoofing) another's identity to hijack the access permissions allocated to another device. In such an environment, it is sufficient to allocate access privileges to each device that selectively allow and prevent devices from accessing portions of a resource according to the allocated access privileges, a process referred to as *authorization.*

1045630.1

In an untrusted network, the network may be widely distributed and the devices on the

network may be unknown to the owner of the resource, making the network vulnerable to

intruders or other bad actors (see e.g., Yu, cols. 8 and 9). Accordingly, authorization may not be

sufficient because a request representing itself as being from a particular device cannot be trusted

to have genuinely been sent from that device rather than from another device attempting to spoof

its identity to gain unauthorized access to information. Accordingly, Yu implements

authentication techniques to verify that a device is actually the device it represents itself to be,

thus preventing unauthorized access to a resource via spoofing or capability theft.

It should be appreciated from the foregoing that *authorization* and *authentication* are two

distinct security measures that address separate and distinct security issues. Authentication

techniques are unnecessary in a trusted environment and do not serve to increase security, but

rather add unnecessary complexity to the access management scheme in a trusted environment.

Nowhere does Ericson describe untrusted environments or any type of security breaches

requiring authentication, and the Office Action points to no such teaching. Rather, the Office

Action points out that Ericson mentions that "conventionally known peripheral connection

interfaces ("PCI") and Fibre Channel protocols may be utilized" (col. 6, lines 4-6), and asserts

that this is a teaching that Ericson teaches the use of the disclosed techniques in an untrusted

environment. However, that is an entirely unsupported leap from the mere mention that the

Ericson authorization mechanism can be implemented using a particular protocol. Ericson

mentions Fibre Channel merely to illustrate that the invention can be implemented using

different protocols. Fibre Channel can be used to implement networks in a trusted environment,

and the Office Action does not even attempt to allege otherwise. Thus, the Office Action's

assertion that the mere mention of the Fibre Channel protocol (which is entirely consistent with a

trusted environment) somehow provides a teaching that the Ericson system be used in an

untrusted environment so that security measures of the type used in Yu should be considered is

entirely unsupported.

Nothing is mentioned to suggest that the Eriscon system, even if implemented using the

Fibre Channel protocol, would be used in an untrusted environment. Ericson is completely silent

1045630.1

with respect to security risks in widespread networks, the dangers of environments that are vulnerable to spoofing, or any other disclosure that would have motivated one skilled in the art to seek security measures that would be useful in an untrusted network but entirely unnecessary in a trusted environment. Furthermore, not only is Ericson silent about an untrusted environment, but Ericson's entire description is in the context of a trusted environment. In particular, the controlled data storage access system of Ericson is performed in a SCSI environment where initiators are trusted. As discussed below, both the nature of the SCSI environment and the details of the SCSI interface make it unnecessary and therefore undesirable to implement verification or authentication methods as disclosed by Yu.

The SCSI protocol defines a standard for communication between a computer and various peripheral devices. In particular, various host devices (referred to as initiators) may issue requests to one or more peripheral devices (referred to as targets) that are connected to the SCSI bus. Each device (i.e., an initiator or a target) has a unique SCSI ID which identifies its physical location on the SCSI bus. The narrow SCSI bus and associated connectors support a maximum of eight devices. The wide SCSI bus and associated connectors support a maximum of 16 devices. See e.g., http://scsifaq.paralan.com/ and, in particular, http://scsifaq.paralan.com/scsifaqanswers.html#9 and http://scsifaq.paralan.com/scsifaqanswers.html#10.

The SCSI environment is local and contained, and therefore trusted and secure. Only a limited number of devices can be attached to a SCSI bus over a limited and local area. For example, internal SCSI connections (i.e., SCSI ribbon connections) are designed for communication between components and peripherals within the same computer (e.g., a personal computer). See e.g., http://computer.howstuffworks.com/scsi5.htm. External SCSI connections (i.e., SCSI cables) are designed to connect peripherals over relatively short distances. For example, SCSI cables typically come in 3ft and 6ft lengths. Although the cables may be daisy-chained, the SCSI protocol itself does not support bus lengths greater than 25 meters.

1045630.1

Accordingly, a SCSI network is limited to a small area and limited to a small number of devices. See e.g., http://www.ramelectronics.net/html/scsi_connecters.html#cablelength.

In addition, each device on the SCSI bus must be manually configured and physically connected to the bus via an appropriate SCSI connector, and assigned a unique SCSI ID (often by manually setting a physical switch or configuring external jumpers). To assign a unique SCSI ID to a device (i.e., 0-7 for narrow SCSI and 0-15 for wide SCSI), the SCSI ID of every other device on the bus must be known to avoid conflicts. See e.g., http://computer.howstuffworks.com/scsi3.htm; http://support.gateway.com/s/CDROM/Panasonc/CS006aa/PANAS100.shtml.

Accordingly, there are no unknown or untrusted devices connected to a SCSI bus. An operator or administrator building a SCSI network must physically attach each device to the bus and configure it appropriately. http://www.sun.com/solutions/blueprints/0800/scsi.pdf (see especially "SCSI Issues in Clusters" on page 3, et. seq.) Therefore, the operator is cognizant of each device on the network and is fully in control of what devices are connected to the SCSI bus. That is, untrusted devices cannot gain access to the SCSI bus. In such a local and trusted environment, it would have been unnecessary to implement verification and/or authentification procedures.

Furthermore, the SCSI interface itself prevents a device from misrepresenting its identity. The SCSI ID assigned to each device connected to a SCSI bus both identifies the device and specifies the device's physical address on the bus. The uniqueness of a SCSI ID is a requirement of the interface. http://www.sun.com/solutions/blueprints/0800/scsi.pdf. For example, bus arbitration and communication depends on each attached device having a unique SCSI ID. Conflicts with SCSI IDs prevent the conflicting devices from gaining access and communicating over the SCSI bus (and may result in the failure of all devices on the SCSI bus). http://www.ba-stuttgart.de/~schulte/htme/ebuss12.htm#REF2.1.2. The uniqueness of a device's SCSI ID is its license to access the bus. For a device to communicate over the bus, it must represent itself by that unique SCSI ID. Accordingly, there is no way for a device to misrepresent itself without disrupting the SCSI network.

1045630.1

In Ericson, a plurality of initiators 100 are connected via a SCSI bus 104 to a target device 102 such as a disk array having a controller 106 (col. 3, line 53 – col. 4, line 5). Upon request by an initiator, the controller accesses a look-up data structure that defines which initiators have access to which logical units of the disk array to ensure that the request is permitted (col. 4, lines 6-54). In Ericson, the allocation of logical units to particular initiators is conducted in a trusted environment. For example, column 4, lines 54-61 state:

> The look-up data structure may be pre-configured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. This preconfiguration preferably is performed when the target controller 106 is installed. When necessary, however, the look-up data structure may be reconfigured at any subsequent time, such as when new initiators 100 are added to the system, or when the logical units 108 must be reassigned to other initiators 100.

The system operator is in complete control of the local SCSI network. The system operator configures the look-up data structure according to the devices on the SCSI bus and allocates logical units to new devices added onto the SCSI bus as desired. The system operator is trusted with properly adding devices to the SCSI bus and defining the look-up data structure to permit access as desired by associating initiator IDs with desired logical units. In a SCSI environment, the system operator must give each device a unique SCSI ID which must remain unique in order for a device to communicate on the bus.

In this environment, there is no opportunity for a device to misrepresent its identity to gain access to restricted logical units of the target device. The SCSI network is a local and contained network of devices wherein the administrator of the network has control over connecting each of the devices, configuring their SCSI ID's and allocating their respective permissions. Not only are there no untrusted devices on the SCSI network, but the SCSI network itself prevents devices from spoofing their identity to gain access credentials of another device.

While Ericson mentions that other peripheral interfaces (e.g., Fibre Channel) may be used, Ericson does not contemplate untrusted environments or anywhere suggest that the described access method could be used in environments where there is a possibility that initiators may attempt to misrepresent their identity to gain access to restricted logical units. In particular,

nowhere does Ericson disclose an environment where untrusted devices have access to the data storage, nor does Ericson suggest that spoofing is, or would be, a problem. Accordingly, authenticating the identity of a device is completely unnecessary in Ericson.

> iii.   *Boggs Adds Nothing To Support Motivation for Modifying Ericson In View of Yu*

The 4/21/06 Office Action asserts that "It is well known in the art at the time of the invention that SCSI peripherals may be distributed over wide area network using ATM Fibre Channel. See for example Boggs et al. US Patent 5,959,994 col. 2 lines 63-68, col. 10 lines 8-22)." (Office Action, page 3). Initially, Applicants respectfully traverse this assertion regarding what was purportedly well known, so that if this assertion is to be relied upon, Applicants request that a reference be cited to support it.

The above-quoted assertion in the Office Action is a bit unclear as to exactly what teaching allegedly embodied therein the Examiner believes would have motivated one of skill in the art to modify Ericson to employ security techniques only useful in an untrusted environment, but it is respectfully asserted that the assertion is based upon a misunderstanding of what is disclosed in Boggs.

The only figures of Boggs that disclose the use of a SCSI bus are Figs. 11-12 that illustrate prior art systems. In those figures, a configuration is shown wherein a number of disk arrays 1222-1228 are connected to a number of processing systems 1202-1208 via a SCSI bus 1230. The processing systems are connected via a local area network (LAN) 1212 to clients. It should be appreciated that the communication between the clients and the processing systems 1202-1208 does not occur over the SCSI bus 1230. Thus, to the extent the Office Action asserts that such communications are untrusted, then even if that were true, it would have no impact on the trusted communications over the SCSI bus 1230 between the processing systems 1202-1208 and the disk arrays 1222-1228.

To the extent that Boggs teaches the use of ATM to communicate with the disk arrays 122-126 (Fig. 1), it teaches that ATM replace the use of the SCSI bus to communicate between the disk arrays and the processing systems.

1045630.1

Referring specifically to the passages cited in the Office Action, the first passage (at col. 2, lines 63-68) says nothing more than that Fibre Channel is becoming a more popular peripheral interconnection technology than the parallel SCSI bus. Certainly, nothing can be taken from that statement suggesting that the system of Ericson that employs a SCSI bus is somehow an untrusted environment.

Similarly, the disclosure at col. 10, lines 8-22 indicates that ATM is a preferred universal interconnect for peripherals, and that it can be adapted to use the SCSI Fibre Channel protocol (FCP), which is the serial SCSI protocol supported by Fibre Channel. The fact that the Fibre Channel standard can be adapted to support the SCSI protocol says nothing at all to suggest that the trusted environment of Ericson could somehow be untrusted.

In view of the foregoing, there is simply nothing in Boggs to suggest that the environment of Ericson is untrusted and would benefit from the type of security techniques taught by Yu.

iv.   Summary of Arguments Regarding Ericson and Yu

In the "Response to Arguments" section, the 9/19/05 Office Action asserts on page 2 that the motivation to combine Ericson and Yu is that Ericson benefits from "the advantage of [Yu's] security method." As discussed above, the Office Action has the burden of showing that authentication is in fact an advantage in Ericson. In order for the Office Action's assertion to operate as valid motivation to combine Ericson and Yu, the Office Action must demonstrate that there is a threat in Ericson that would justify adding authentication security measures. Absent a security threat that would be remedied by authentication, one of ordinary skill in the art simply would not have been motivated to add unnecessary complexity and expense. Analogously, no one would be motivated to purchase snow tires for their car in Southern California. It is senseless to protect against non-existent threats.

Applicant has produced evidence that there is in fact no security threat in Ericson that would be remedied by Yu's authentication. However, it is not Applicant's burden to conclusively establish the absence of a threat in Ericson that could be remedied by authentication, as it is the Office Action's burden to prove that such a threat exists in Ericson.
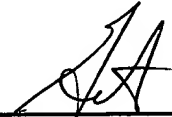
1045630.1

The Office Action has failed to produce any such evidence, and therefore has failed to establish a *prima facie* case of obviousness. Accordingly, Applicant respectfully requests that the rejection be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,
Steven M. Blumenau et al., Applicant

By: _____

Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No.E0295.70066US00
Date: July 17, 2006
x

1045630.1